The New York Times

Too Many New Gadgets, Too Much Information at Risk

By DAVID S. JOACHIM
Published: February 21, 2006

It is the corporate version of keeping up with the Joneses: every day, it seems, someone arrives at the office with a shiny new gadget that combines a cellphone with all sorts of features you used to find only on your computer. They can get e-mail messages, surf the Web, manage contact lists and calendars, and even create Word and Excel documents that can run on a conventional PC.

These smart phones and hand-held computers are so powerful that many office workers now travel without their laptops. Why bother with a clunky box that takes several minutes to start up and connect to a network, when you have a device that is always online and can access information on demand?

At first, owners and operators of small businesses may see benefits to this trend. After all, workers are paying for their own little devices in the name of convenience. But, it turns out, they are also giving their technology departments a big headache.

That is because these devices represent a sizable security risk. For one, they are configured to hop from Wi-Fi to cellular networks easily, exposing them to deliberate thievery of data. But a bigger threat, analysts say, is that small things are easier to lose, raising the prospect that confidential business files will get in the wrong hands.

Pocket-size devices are misplaced all the time — travelers left 85,000 cellphones and 21,000 hand-held computers in Chicago taxis during a six-month period last year, according to a survey by Pointsec Mobile Technologies, a maker of security software. And as these devices become capable of storing larger volumes of data, some experts are concerned about the increasing vulnerability of those files.

Analysts say that workers are too caught up with buying the latest gadgets, forgetting that their data is far more valuable than the device it runs on.

That is why some companies, realizing the potential for damage, are getting ahead on mobile security by actually buying small gadgets for their employees, albeit with security strings attached. Seitlin, a small insurance brokerage based in Miami, illustrates the point.

The firm decided to buy Palm Treo cellphone-organizers for about 30 of its 250 employees. The company could then dictate what data was stored on the devices, and it could install software to monitor them from afar and even lock them over the air if they fell into the wrong hands, said Ed Whipple, the

company's vice president for sales and technology.

Seitlin sales agents, rather than carry client records on their Treos, must use a Web site to access claims histories and other private information. These files can be viewed but not stored on the devices through an online service called Nexsure from XDimensional Technologies. If an agent on the road is offline and needs information about a client, he calls the office for it, Mr. Whipple said.

If an employee reports that his cellphone is stolen, Mr. Whipple can send a text message to the device, which locks it and asks for a security code, using software called Butler. If the security code is not entered immediately, the memory on the device is wiped clean.

The catch is that the Treo must be turned on and transmitting over a wireless or cellular network for Butler to work. For this reason, some companies set up their devices to store all data on a removable SD memory card, which scrambles the data and renders it useless if the card is removed.

Seitlin also uses software from Intellisync that allows Treos to act like BlackBerry devices and automatically send e-mail messages without the user having to manually download them. This also allows the devices to stay synchronized with a server in the office.

"That's the beautiful thing," Mr. Whipple said. "If I drop my Treo in the water tomorrow, I can go out and buy another one,"

and the technology department can rebuild the software on a new one to look just like the old one, including all his personal contacts and calendars. This can be done in minutes over the air.

John Pescatore, a security analyst at Gartner, a market research company, said that forcing all users to synchronize their data to a single server over the air has another benefit over letting them use their office PC's for backing up data: it creates a log of all information moving to and from the devices. Monitoring software can be set up to search through the data exchanges to make sure no confidential data passes to unauthorized devices, he said.

Mr. Pescatore expects this year to be a turning point for mobile security, in the same way that personal firewalls and antivirus software on PC's gained importance early in the decade because of viruses like I Love You and Melissa. "The market doesn't demand security until something bad happens," he said.

Of course, security breaches get the most attention when they happen at big companies. But as hardware and software prices have dropped in recent years, small businesses are catching up to larger ones in terms of technology — and vulnerability.
By the end of the year, smart phones with so much storage and processing power will represent about half of all cellphones in the United States, compared with about 30 percent today, Mr. Pescatore said. The proliferation could get people in the habit of sending one another executable files like games, which can carry viruses.

More than that, the success of devices that use Microsoft's mobile operating system will mean a decline in the diversity of software, Mr. Pescatore added. Just as Microsoft's domination in PC's made it attractive for programmers to write viruses for Windows, the same could happen to hand-held devices.
In computing, as in nature, diversity is the great inoculator.